CLAIMS

WHAT IS CLAIMED IS:

1. A method for controlling access to information from a DNS server having an access control list specifying clients approved to receive an IP address corresponding to a domain name of a target host, the method comprising:

receiving a request from a client for an IP address of a domain name at the DNS server;

looking up the domain name in the access control list; and

sending to the client a reply containing the IP address of the domain name if the client is authorized in the access control list to receive the IP address, and denying said request if the client is not authorized to receive the IP address.

2. The method of claim 1 wherein sending a reply to the client comprises sending an encrypted reply.

3. The method of claim 2 wherein the authorized clients have access to a decryption key.

4. The method of claim 2 wherein receiving a request comprises receiving a nonsecure request.

5. The method of claim 2 wherein receiving a request comprises receiving an encrypted request.

6. The method of claim 2 wherein receiving a request comprises receiving a signed request.

7. The method of claim 6 further comprising verifying the signature to authenticate the client sending the request.

8. The method of claim 1 wherein receiving a request comprises receiving the request from a second DNS server.

9. The method of claim 8 wherein sending a reply comprises sending an encrypted reply and wherein the second DNS server is configured to forward the reply to the client and is not configured to read the encrypted reply.

10. The method of claim 1 further comprising distributing decryption keys to the clients authorized in the access control list to receive the IP address of the target host.

11. The method of claim 1 further comprising selecting a security level for the reply.

12. The method of claim 11 wherein selecting the security level comprises selecting a default security level based on the security level of the request.

13. The method of claim 1 wherein receiving a request comprises receiving a request over the Internet.

14. The method of claim 1 wherein all clients are authorized to receive the IP address of the domain name if no clients are listed in the access control list for the domain name.

15. The method of claim 1 wherein receiving a request comprises receiving a URL at the DNS server, the IP address corresponding to the URL.

16. The method of claim 2 wherein the authorized clients have access to a signature key.

17. The method of claim 1 further comprising distributing signature keys to the clients authorized in the access control list to receive the IP address of the target host.

18. A computer program product for controlling access to information from DNS server having an access control list specifying clients approved to receive an IP address corresponding to a domain name of a target host, the product comprising:

computer code that receives a request from a client for an IP address of a domain name at the DNS server;

computer code that looks up the domain name in the access control list;

computer code that sends to the client a reply containing the IP address of the domain name if the client is authorized in the access control list to receive the IP address, and denies said request if the client is not authorized to receive the IP address; and

a computer-readable storage medium for storing the codes.

19. The computer program product of claim 18 wherein the computer readable medium is selected from the group consisting of CD-ROM, floppy disk, tape, flash memory, system memory, hard drive, and data signal embodied in a carrier wave.

20. The computer program product of claim 18 further comprising code that encrypts the reply.

21. The computer program product of claim 18 further comprising code that verifies a digital signature sent from the client with the request.

22. A system for controlling access to information from a DNS server, the system having a DNS server comprising:

an access control list specifying clients approved to receive an IP address corresponding to a domain name of a target host;

a processor configured to receive a request from a client for an IP address of the domain name, look up the domain name in the access control list, and send the client a reply containing the IP address of the domain name if the client is authorized in the access control list to receive the IP address, and deny said request if the client is not authorized to receive the IP address; and

memory for storing the access control list, domain names, and corresponding IP addresses.

23. The system of claim 22 wherein the reply is encrypted.

24. The system of claim 23 wherein the clients authorized in the access control list to receive the IP address of the domain name have access to a decryption key.

25. The system of claim 23 wherein the request is a nonsecure request.

26. The system of claim 23 wherein the request is encrypted.

27. The system of claim 22 wherein the DNS server is configured to receive recursively forwarded requests from a second DNS server and send replies to the second DNS server.

28. The system of claim 27 wherein the second DNS server is configured to forward the reply to the client and is not configured to read the encrypted reply.

29. The system of claim 22 wherein the processor is configured to determine whether the reply is to be sent encrypted.

30. The system of claim 22 wherein the processor is configured to verify a digital signature contained within the request.

31. The system of claim 30 wherein the client is only authorized to receive the IP address if the signature is verified.

32. The system of claim 22 wherein a reply is sent to any client requesting the IP address of a domain name having no specified clients in the access control list.

33. The system of claim 22 wherein the domain name is a URL.

34. The system of claim 23 wherein the clients authorized in the access list to receive the IP address of the domain name have access to a signature key.